AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means ☑ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Western District of Pennsylvania

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* BLACK CLOUD MOBILE CELLULAR PHONE (TARGET DEVICE)	)	Case No. 24-1258

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Western District of Pennsylvania *(identify the person or describe the property to be searched and give its location)*:

Please see Attachment A, incorporated herein.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

Please see Attachment B, incorporated herein.

YOU ARE COMMANDED to execute this warrant on or before August 6, 2024 *(not to exceed 14 days)*

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Duty Magistrate Judge.

(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: July 24, 2024 @ 8:30 am

Judge's signature

City and state: Pittsburgh, Pennsylvania

Hon. Patricia L. Dodge, U.S. Magistrate Judge

Printed name and title

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

Return

Case No.: 24-1258	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

Print Save As... Reset

ATTACHMENT A

Property to Be Searched

The item to be searched is:

TARGET DEVICE: Black Cloud Mobile Cellular Phone

The Target Device will be charged and powered on. The device(s) and all readable and searchable contents will be downloaded to a "CelleBrite" or "XRY" or similar device. The contents downloaded on the "CelleBrite" or "XRY" or similar device will then be copied to a readable computer disc and reviewed by your Affiant or other investigators participating in the investigation. A search warrant return will be provided to the Court thereafter. The **TARGET DEVICE** are currently located in the evidence storage facilities at FBI Pittsburgh, 3311 East Carson Street, Pittsburgh, Pennsylvania 15203, and are stored in a manner that is designed to preserve the electronic data.

ATTACHMENT B

Property to be Seized

II. CELLULAR TELEPHONES

1. All records on cellular telephones that relate to violations of Title 21, United States Code, Sections 841, 843(b), and 846 and Title 18, United States Code, Sections 922(g)(1) and 924(c) including:

a. Evidence of communications referring to or relating to illegal narcotics or narcotics trafficking, including records of telephone calls, emails, instant messaging, or other records of communications, and including the identity of phone numbers, email accounts, or other electronic accounts used for such communications;

b. Evidence of communications with suppliers, purchasers, prospective suppliers, or prospective purchasers of illegal narcotics, including records of telephone calls, emails, instant messaging, or other records of communications, and including the identity of phone numbers, email accounts, or other electronic accounts used for such communications;

c. Evidence of communications referring to or relating to firearms and/or ammunition, including records of telephone calls, emails, instant messaging, or other records of communications, and including the identity of phone numbers, email accounts, or other electronic accounts used for such communications;

d. Documents, including photographs and video, depicting illegal narcotics, drug paraphernalia, firearms, or ammunition;

e. Documents, including video and/or audio recordings, discussing and/or referring to illegal narcotics, drug paraphernalia, firearms, or ammunition;

f. Documents, including photographs and video, depicting illegal narcotics, drug paraphernalia, firearms, ammunition, violence relating to firearms or ammunition;

g. Any and all information revealing the identity of co-conspirators in drug trafficking and/or firearm-related activity;

h. Any and all bank records, transactional records, records of wire transfers, checks, credit card bills, account information, and other financial records;

i. Any and all information suggesting sudden or unexplained wealth and/or unidentified conspirators;

j. Any and all information identifying the sources of supply and/or unidentified conspirators may have secured illegal narcotics, drug paraphernalia, firearms, and/or ammunition; and

k. Any and all information recording the scheduling of travel and/or unidentified conspirators, including destinations, dates of travel, and names used during travel.

2. All text messaging, call logs, emails, and/or other records of communication relating to the planning and operation of drug trafficking, misuse of communications facilities, illegal possession of firearms, and possession of firearms in furtherance of drug trafficking crimes, in violation of 21 U.S.C. §§ 841, 843(b), and 846 and 18 U.S.C. §§ 922(g)(1) and 924(c).

3. Evidence of user attribution showing who used, owned, or controlled the cellular telephones at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence.

4. Evidence of software that would allow others to control the cellular telephones, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software.

5. Evidence of the lack of such malicious software.

6. Evidence indicating how and when the cellular telephones were accessed or used to determine the chronological context of the cellular telephones access, use, and events relating to the crimes under investigation and to the cellular telephones user.

7. Evidence indicating the cellular telephones user's state of mind as it relates to the crime under investigation.

8. Evidence of the attachment to the cellular telephones of other storage devices or similar containers for electronic evidence.

9. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the cellular telephones.

10. Evidence of the times the cellular telephones were used.

11. Evidence of how the cellular telephones were used and the purpose of its use including firewall logs, caches, browsing history, cookies, "bookmarked" or "favorite" web pages, temporary Internet directory or "cache," search terms that the user entered into any Internet search engine, records of user-typed web addresses, and other records of or information about the cellular telephones' Internet activity.

12. Records of or information about Internet Protocol addresses used by the cellular telephones.

13. Passwords, encryption keys, and other access devices that may be necessary to access the cellular telephones.

14. Documentation and manuals that may be necessary to access the cellular telephones or to conduct a forensic examination of the cellular telephones.

15. Contextual information necessary to understand the evidence described in this attachment.

16. All serial numbers or International Mobile Equipment Identity (IMEI) numbers associated with any cellular telephones.

17. Log files, contact information, phone books, voicemails, text messages, draft messages, other stored communication, calendar entries, videos, and photographs related to matters described above.

In searching the cellular telephones, and during the execution of these search warrants, law enforcement is permitted to: (1) depress WILLIAM's thumb- and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of WILLIAMS' face with his eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force; specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

In searching the cellular telephones, the federal agents may examine all of the information contained in the cellular telephones to view their precise contents and determine whether the cellular telephones and/or information fall within the items to be seized as set forth above. In addition, they may search for and attempt to recover "deleted," "hidden," or encrypted information to determine whether the information falls within the list of items to be seized as set forth above.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any of the following:

a. Any form of computer or electronic storage (such as hard disks or other media that can store data);

b. Text messages or similar messages such as SMS or IM, saved messages, deleted messages, draft messages, call logs, all phone settings (*i.e.* call, messaging, display), priority senders, photographs, videos, links, account information, voicemails and all other voice recordings, contact and group lists, and favorites;

c. Pictures, all files, cloud files and relevant data without password access, storage information, documents, videos, programs, calendar information, notes, memos, word documents, PowerPoint documents, Excel Spreadsheets, and date and time data;

d. Payment information, to include account numbers, names, addresses, methods of payment, amounts, additional contact information, and financial institutions;

e. Lists and telephone numbers (including the number of the phone itself), names, nicknames, indicia of ownership and/or use, and/or other contact and/or identifying data of customer, co-conspirators, and financial institutions;

f. Applications (Apps), to include subscriber information, provider information, login information, contact and group lists, favorites, history, deleted items, saved items, downloads, logs, photographs, videos, links, messaging or other communications, or other identifying information;

g. Social media sites to include, name and provider information of social media network(s), profile name(s), addresses, contact and group lists (*i.e*. friends, associates, etc.), photographs, videos, links, favorites, likes, biographical information (*i.e*. date of birth) displayed on individual page(s), telephone numbers, email addresses, notes, memos, word documents,

downloads, status, translations, shared information, GPS, mapping, and other information providing location and geographical data, blogs, posts, updates, messages, or emails;

h. Any information related to co-conspirators (including names, addresses, telephone numbers, or any other identifying information);

i. Travel log records from GPS data (*i.e.* Google Maps and/or other Apps), recent history, favorites, saved locations and/or routes, settings, account information, calendar information, and dropped pinpoint information;

j. Internet service provider information, accounts, notifications, catalogs, Wi-Fi information, search history, bookmarks, favorites, recent tabs, deleted items and/or files, downloads, purchase history, photographs, videos, links, calendar information, settings, home page information, shared history and/or information, printed history and/or information, or location data;

k. Email data, including email addresses, IP addresses, DNS provider information, telecommunication service provider information, subscriber information, email provider information, logs, drafts, downloads, inbox mail, sent mail, outbox mail, trash mail, junk mail, contact lists, group lists, attachments and links, and any additional information indicative of operating a sophisticated fraud scheme, or other criminal violations;

l. Any handmade form (such as writing);

m. Any mechanical form (such as printing or typing); and

n. Any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).